Телекомунікаційною основою для системи електронного документообігу може стати спеціальна інформаційно-телекомунікаційна система, що розгорнута в межах Національної системи конфіденційного зв'язку. Забезпечується цілісність загальнодержавного елетронного документообігу і захищеність інформаційного обміну.

У світі почалася «нова ера кібертероризму», що є наслідком глобального процесу інформатизації, та охоплює всі сфери життя. Люди дедалі більше усвідомлюють факт переміщення загроз у кіберпростір. Кібертероризм - це сукупність організованих несанкціонованих дій, спрямованих на порушення штатного режиму функціонування інформаційно-телекомунікаційних систем та порядку обробки інформаційних ресурсів. Це робиться з метою отримання несанкціонованого доступу або виведення таких систем з ладу.

Вирішення цих завдань потребує підвищення якості підготовки кадрів та відповідного законодавчого забезпечення, а також особливої уваги з боку держави для прискорення процесів створення осередків протидії кібертероризму в Україні.

Порядок надання користувачу інформації з вказаними місцем, часом, відповідальними посадовими особами, а також необхідними процедурами встановлює власник документів, масиву документів та інформаційних систем або вповноважені ним особи відповідно до чинного законодавства, а також забезпечує умови доступу користувачів до інформації. Власник документів, масиву документів та інформаційних систем забезпечує рівень захисту інформації згідно з законодавством України.

Список літератури

1. Гайкович В, Першин О. Безпека електронних банківських систем. - М., 1999.
2. Карасик І. Програмні та апаратні засоби захисту інформації для персональних комп'ютерів // КомпьютерПресс. – № 3, – 1995
3. Петров В.А., Піскарьов С.А., Шеїн А.В. Інформаційна безпека. Захист інформації від несанкціонованого доступу в автоматизованих системах. – М., 1998.

УДК 004.4

Д.В. Гладишев
Науковий керівник – Смірнов О.А., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Розробка програмного забезпечення захисту конфіденційної інформації у мережі методом стеганографії

Тема, обрана для дослідження, є актуальною у зв'язку з бурхливим розвитком комп'ютерних технологій і впровадження їх у повсякденне життя. Одна з основних проблем такого розвитку суспільства є проблема захисту інформації. Стеганографія вирішує такі гострі питання як: електронно-цифровий підпис, захист прав інтелектуальної власності й авторських прав, а також сховане зберігання й передача секретної (закритої) інформації з відкритих каналів передачі даних. Математичні аспекти цієї проблематики на сьогоднішній день розроблені недостатньо й дане дослідження деякою мірою заповнює цей пробіл.

Існує два принципово різних способи передачі по відкритому каналу зв'язку конфіденційної (секретної) інформації. Перший з них, відомий як шифрування, складається в заміні (по деякому алгоритму) символів переданої інформації іншими

символами, у результаті чого виходить шифртекст, що і спостерігається «супротивником» у каналі зв'язку. Наука, що вирішує відповідні проблеми забезпечення безпеки переданої таким способом конфіденційної інформації, називається криптографією.

Другий спосіб полягає в тому, щоб замаскувати передану секретну інформацію іншою, так званою, «шумовою» інформацією, що звичайно являє собою переданий по каналу зв'язку деякий відкритий текст. У цьому випадку секретні символи «вкрапляються» у відкритий текст, тобто деякі його знаки заміняються на «секретні» знаки. Такий, видозмінений відкритий текст, що несе в собі секретну інформацію, і спостерігається «супротивником». Відповідна наука про організацію й аналіз подібних процедур приховання інформації називається стеганографією.

Треба відзначити, що якщо криптографія, як математична наука, є в цей час досить просунутою, те цього не можна сказати про стеганографію. Тут на сьогодні досить добре розроблені відповідні технологічні аспекти; що ж стосується побудови й аналізу адекватних математичних моделей, те ці питання ще чекають свого кваліфікованого рішення, і сьогодення дослідження має своєю метою в певній мері усунути наявний тут пробіл.

Криптографічний захист інформації не знімає проблему приховання конфіденційної інформації повністю, оскільки наявність шифрованого повідомлення вже саме по собі привертає увагу «супротивника», і він, заволодівши криптографічно захищеним файлом, відразу виявляє факт розміщення в ньому секретної інформації й може кинути всю сумарну міць своєї комп'ютерної бази на дешифрування схованих даних. Тому для передачі конфіденційної інформації широко використовують також і стеганографічні методи.

Термін «стеганографія» походить від двох грецьких слів – steganos (таємниця) і graphy (запис), тому її можна називати тайнописом. Хоча термін «стеганографія» з'явився тільки наприкінці XV століття, використовувати стеганографію почали кілька тисячоріч тому. Стеганографія – це наука про сховану передачу інформації шляхом збереження в таємниці самого факту передачі секретних даних. На відміну від криптографії, що приховує вміст секретного повідомлення, стеганографія приховує саму його наявність. Стеганографія не заміняє, а доповнює криптографію. Приховання повідомлення методами стеганографії значно знижує ймовірність виявлення самого факту передачі конфіденційного повідомлення, а якщо це повідомлення до того ж і зашифроване, то воно має ще один, додатковий, рівень захисту.

Стеганографія – це метод організації зв'язку. Завданням стеганографії є приховання самого факту існування секретних даних при їхній передачі, зберіганні або обробці. Інакше кажучи, під прихованням існування інформації мається на увазі не тільки неможливість виявлення в перехопленому повідомленні схованого повідомлення, але й взагалі унеможливити виникнення будь-яких підозр на цей рахунок. Загальною рисою стеганографічних методів є те, що приховуване повідомлення вбудовується в якийсь, не приваблюючий уваги, об'єкт (контейнер), що потім відкрито пересилається адресатові. На відміну від криптографії, де ворог точно може визначити, чи є повідомлення зашифрованим, методи стеганографії дозволяють вбудовувати секретні повідомлення в необразливі файли так, щоб не можна було запідозрити існування таємного послання.

На сьогоднішній день стеганографічна система, або стегосистема, може розглядатися як сукупність засобів і методів, які використовуються для формування схованого каналу передачі інформації. При побудові стеганографічної системи враховуються наступні положення. Супротивник має повне подання про стеганографічну систему. Єдиною інформацією, що невідома потенційному супротивникові, є ключ, за допомогою якого тільки його тримач може встановити факт присутності повідомлення і його зміст. Таким чином, вся таємність системи захисту

переданих повідомлень повинна втримуватися в ключі – фрагменті інформації, попередньо розділеному між адресатами.

Найбільш перспективним напрямком стеганографії на сьогоднішній день є цифрова стеганографія – напрямок комп'ютерної стеганографії, заснований на прихованні інформації в цифрових об'єктах, що споконвічно мають аналогову природу, тобто мультимедіа-об'єкти (зображення, відео, звуки). У зв'язку з розвитком апаратних засобів обчислювальної техніки й величезною кількістю каналів передачі інформації з'явилися нові стеганографічні методи, в основі яких лежать особливості подання інформації у файлах, обчислювальних мережах і т.п. Таким чином, поряд з добре вивченими математичними моделями криптографії, побудова математичних моделей стеганографії і їхній ймовірносно-статистичний аналіз є актуальною проблематикою.

Метою роботи є побудова програмного забезпечення математичних моделей вбудовування секретної інформації при її зберіганні або передачі по відкритих каналах зв'язку й дослідження стійкості стеганосистеми залежно від кількості вбудовуваємої інформації й особливостей самого процесу вбудовування.

У роботі використовуються методи математичного аналізу, теорії ймовірностей і математичної статистики, теорії цифрової обробки сигналів і зображень.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.

Список літератури

1. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография.– К.: МК-пресс, 2006. – 288 с.
2. Быков С. Ф. Алгоритм сжатия JPEG с позиции компьютерной стеганографии. // Защита информации. Конфидент. – СПб.: 2000, № 3.
3. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганографія. – М.: Солон-пресс, 2002. – 272 с
4. Schneier B (1996) Applied Cryptography. John Wiley and Sons, Indianapolis, IN
5. Dumitrescu, S., W. Xiaolin and Z. Wang, 2003. Detection of LSB steganography via sample pair analysis. In: LNCS, Vol. 2578, Springer-Verlag, New York, pp: 355–372.

УДК 621.391

Ю.М. Козекін

Науковий керівник – Семенов С.Г., канд. техн. наук, ст. наук. співроб., доцент

Національний технічний університет “Харківський політехнічний інститут”

Порівняльний аналіз методів екстраполяції для приховування даних в просторової області нерухомих зображень методом Куттера-Джордана-Боссена

Побудова стеганографічного методу захисту інформації Куттера-Джордана-Боссена заснована на використанні методів екстраполяції (прогнозування) випадкових сигналів.

У доповіді проведено порівняльний аналіз методів екстраполяції та обґрунтовано їх подальше використання у стеганографічних алгоритмах.